

NAPLES COMPUTERS HOW-TO · SECURITY & SAFETY

Phishing Awareness Training for Employees

A ten-minute phishing awareness training for small-business teams, provided by Naples Computers for our clients. It covers what phishing is and why businesses are targeted, the 7 warning signs, the attacks we see most at businesses in Southwest Florida, the Stop-Look-Report rule, how to report phishing in Outlook, what to do if you clicked, and five Phish-or-Legit practice examples. All examples are fictional. A printable quiz, answer key, certificate of completion and desk poster are included.

What is **phishing**?

A message that pretends to be someone you trust, to get you to click, pay, or share.

Email

Fake invoices, password alerts, shared files, messages from “the boss”.

Text messages

Called “smishing”: urgent texts with links or requests.

Phone calls

Called “vishing”: callers posing as I.T., the bank, or a vendor.

Why **your business** is a target

- ☐ Phishing is the #1 reported cybercrime
FBI Internet Crime Report, 2025
- ☐ Business email scams cost about \$3 billion
Reported losses in 2025 alone
- ☐ Attackers target people, not just computers
One convincing message can get past the best filters
- ☐ You are the last line of defense
Pausing for five seconds stops most attacks

The 7 **warning signs**

- ☐ Look-alike sender
yourcompany.com is not yourcompany.com

- ☐ Urgency or threats
"Within 24 hours or else"
- ☐ Generic greeting
"Hello Customer", "Dear user"
- ☐ Links that don't match
Hover first: where does it really go?
- ☐ Unexpected attachments
Especially .html, .zip, or "enable content"
- ☐ Requests for logins or money
Passwords, codes, gift cards, wires
- ☐ Mistakes & odd details
Typos, strange formatting, wrong logos

Business attacks and practice examples

BUSINESS ATTACK 1 OF 6

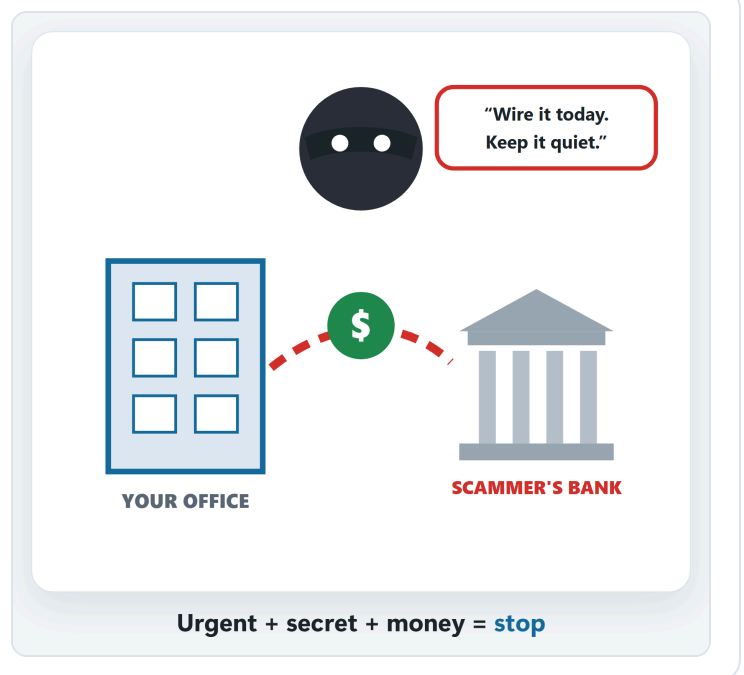


The "boss" or a vendor asks for money

A message that looks like your CEO, owner or a regular vendor asks for a wire transfer, gift cards or a quick payment, often saying they can't talk right now.

WHAT TO DO

Verify every payment request by phone, using a number you already know. Never the number in the message.



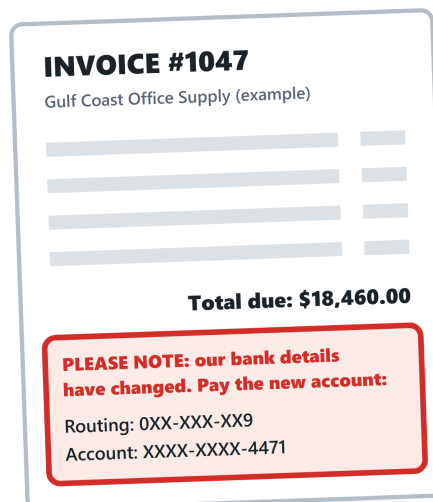
BUSINESS ATTACK 2 OF 6

! Fake invoices and “new bank details”

A real-looking invoice, sometimes from a vendor's hacked email, says their bank account has changed.

WHAT TO DO

Any change to payment details gets a phone call to the vendor, and a second person's approval.



“Our bank details **have changed**”

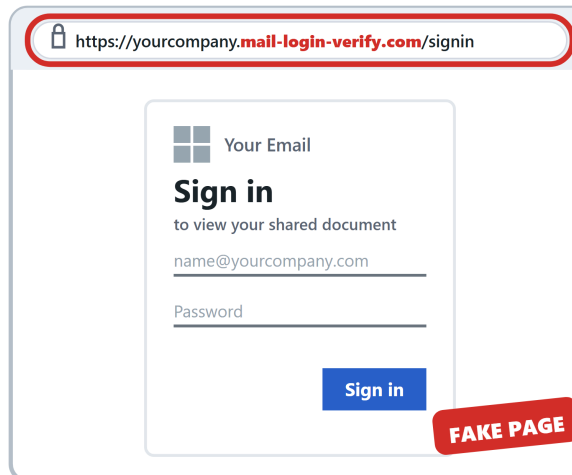
BUSINESS ATTACK 3 OF 6

! Fake Microsoft 365 and email sign-in pages

A link opens a page that looks exactly like your email sign-in page. Anything you type goes to the attacker.

WHAT TO DO

Check the web address before you sign in. When in doubt, close it and go to the site yourself.



Look at the **address bar**, not the logo

BUSINESS ATTACK 4 OF 6



"Someone shared a document with you"

Tempting file names like bonuses, payroll or a voicemail, with a link that asks you to sign in.

WHAT TO DO

Not expecting it? Ask the sender, by phone or chat, before you open it.



Sandra Ruiz shared a file with you



Q4 Bonus Schedule.pdf

Sign in required to view

Open

Link: docs-share-portal.net/view?id=88

Tempting file + strange link

BUSINESS ATTACK 5 OF 6



QR codes that hide the link

A QR code in an email or on a sticker sends you to a fake page on your phone, where it's harder to check the address.

WHAT TO DO

Don't scan QR codes in emails you weren't expecting. Check the address before entering anything.

Action required: re-activate your multi-factor authentication

From: Security Team <it-security@yourcompany-help.com>

Scan the code below with your phone within 24 hours to avoid losing access.



EXAMPLE

A QR code is just a hidden link

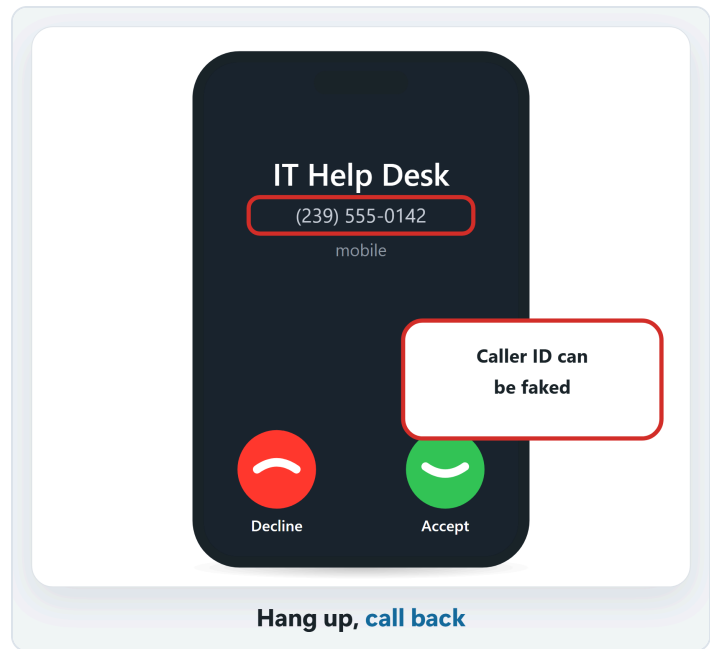
BUSINESS ATTACK 6 OF 6

! Texts and calls from “I.T.” or “the bank”

Caller ID and text names can be faked. Real I.T. and banks won't ask for your password or a sign-in code.

WHAT TO DO

Hang up and call back on a number you know. Never read a code to anyone.



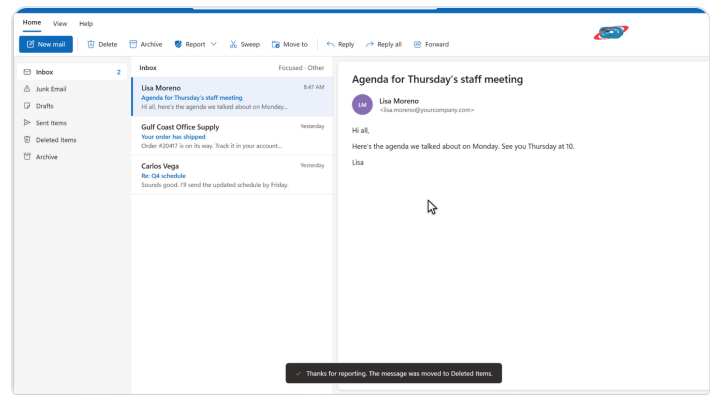
OUTLOOK

! In Outlook: Report → Report phishing

Select the message, then on the Home tab click Report and choose Report phishing.

WHAT TO DO

Confirm with Report. The message is sent to your security team and moved to Deleted Items.



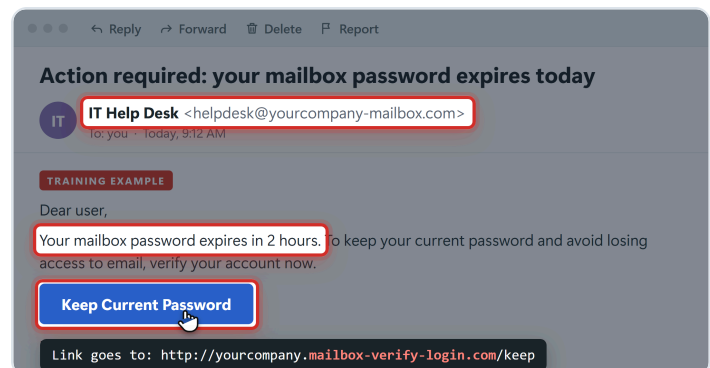
EXAMPLE 1 • PHISH

! A fake password warning

The sender is yourcompany-mailbox.com, not yourcompany.com. It's urgent, and the button leads to a look-alike sign-in page.

WHAT TO DO

Report it. Your real I.T. team won't ask you to “keep your password” through a link.



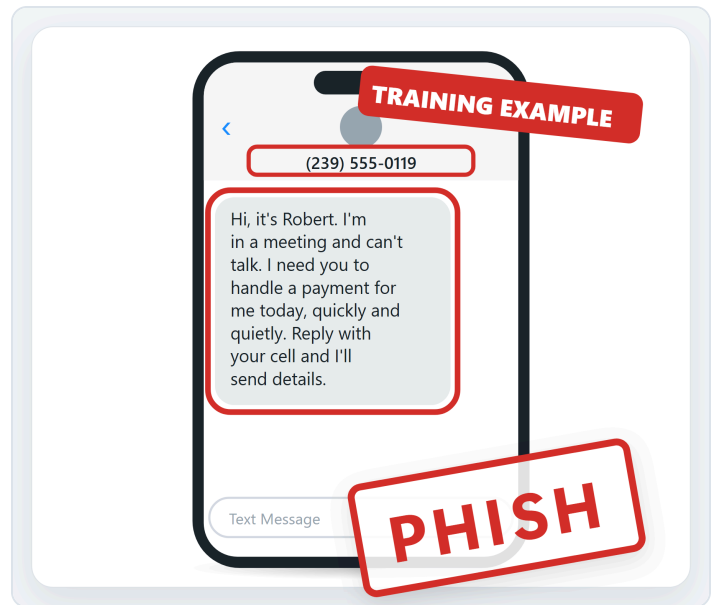
EXAMPLE 2 • PHISH

The “boss” texting from an unknown number

Unknown number, can't talk, urgent and secret, and it's about money. That's a classic business email compromise, by text.

WHAT TO DO

Don't reply. Contact the owner using the number you already have, and tell I.T.



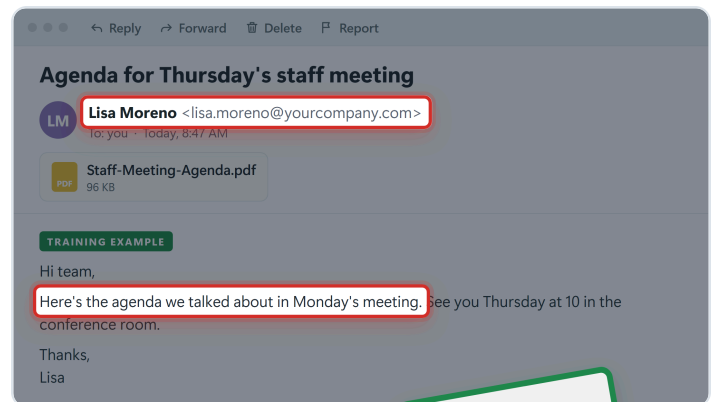
EXAMPLE 3 • LEGIT

An expected email from a coworker

It's from your company's real domain, it mentions a meeting you know about, and it doesn't ask for money, passwords or urgency.

GOOD TO KNOW

Legit. Still, if an attachment ever asks you to “enable content” or sign in, stop and check.



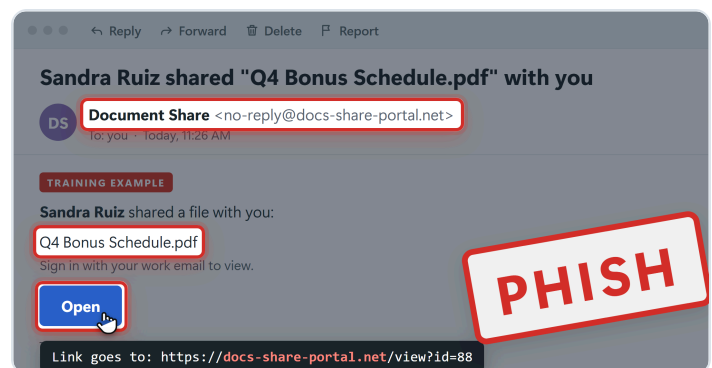
EXAMPLE 4 • PHISH

A tempting shared file

A juicy file name, an outside “document share” address, a link to an unfamiliar site that wants your work sign-in, and a deadline.

WHAT TO DO

Check with the person who supposedly shared it, by phone or chat. Then report it.



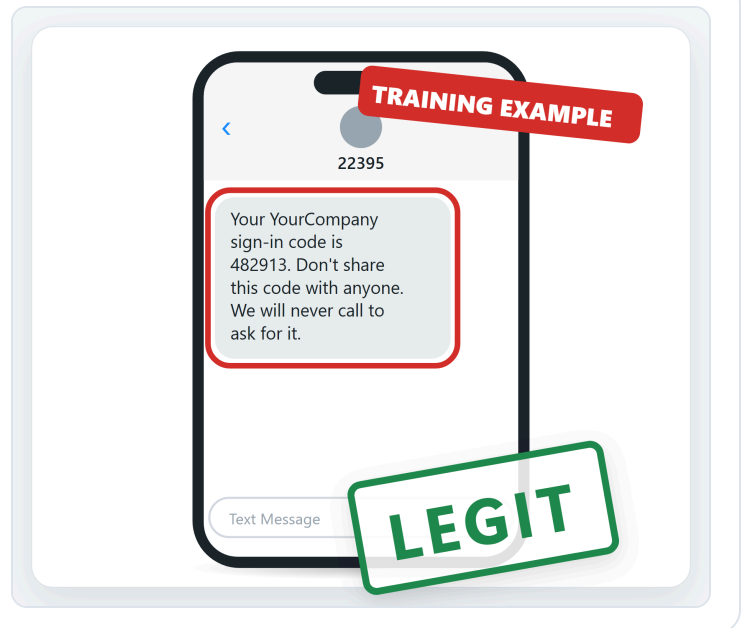
EXAMPLE 5 • LEGIT

! A code you just asked for

You just signed in, the code arrived right away, and it tells you not to share it. That's how real sign-in codes work.

BUT WATCH OUT

Didn't just sign in? Someone may have your password. Don't share the code, change your password, and tell I.T.



The rule: Stop. Look. Report.

- ☐ STOP
Feeling rushed, scared or curious? That's the trap. Pause.
- ☐ LOOK
Sender, links, attachments, the request itself.
- ☐ REPORT
Use the Report button, or tell I.T. Don't just delete it.

No Report button? Tell I.T.

- ☐ Tell your I.T. contact or manager right away
A quick call or chat message is perfect
- ☐ Don't forward it around the office
Asking coworkers "is this real?" spreads the bad link
- ☐ Don't reply, click, or call numbers in it
Even to say "stop"
- ☐ Delete it once it's been reported
Your I.T. team may ask for it first

Clicked? **Speak up, fast.**

- ☐ Tell I.T. immediately
Minutes matter. Nobody is in trouble for reporting.
- ☐ Something downloaded or opened?
Disconnect from the network: unplug the cable or turn off Wi-Fi
- ☐ Typed your password?
Change it right away, from a different device if you can
- ☐ Unexpected sign-in prompts or codes?
Deny them, and never share a code

Reporting fast is never a mistake. Waiting is.

Recap: **Stop. Look. Report.**

- | | |
|--|---|
| ☐ Check the real sender address | ☐ Verify money requests by phone |
| ☐ Urgency and secrecy are red flags | ☐ Never share passwords or codes |
| ☐ Hover before you click; check the address | ☐ Report it; clicked? Tell I.T. fast |

Stop. Look. Report. When a message makes you feel rushed, scared or curious, pause, check the sender and links, and report it. Clicked something? Tell I.T. right away: reporting fast is never a mistake.



Want phishing training, email security or managed I.T. for your business?

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**